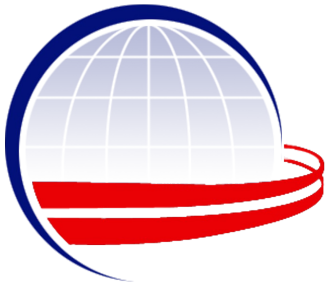
Horizontal Fusion Security Architecture

Les Owens

HF Management Team



HORIZONTAL FUSION

CATALYST FOR NET-CENTRIC TRANSFORMATION • DEPARTMENT OF DEFENSE

HORIZONTAL FUSION

Outline

- **Underlying Security Philosophy**
- **Driving Security Policies**
- **Key Security Technologies**
- **Technical and Security Standards**
- **Conceptual Security Architecture**
- **FY05 and Beyond**

HORIZONTAL FUSION

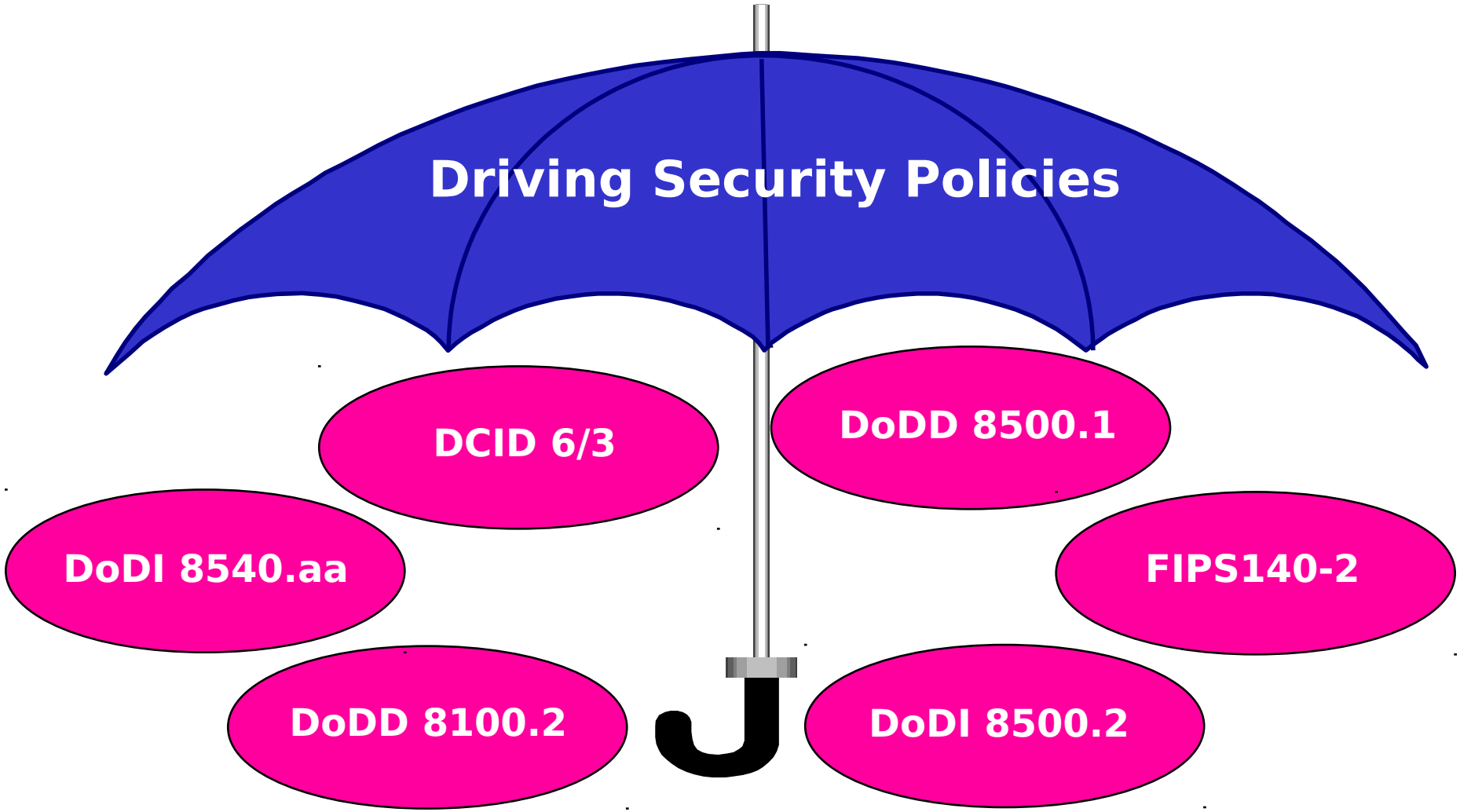
Security Philosophy

- **Build upon Service-Oriented Architecture (SOA)**
- **Extend and adapt commercial best practices to the government Net-centric environment**
- **Use decentralized security to all components of the architecture and move security closer to the edge**
- **Employ security Defense-in-Depth approach**
- **Move away from “the way its always been done”**
- **Prudently apply security policy in a Net-centric environment**

Risk Management not Risk Avoidance

HORIZONTAL FUSION

Major Security Policies Embraced by HF



HORIZONTAL FUSION

Security Roles & Responsibilities

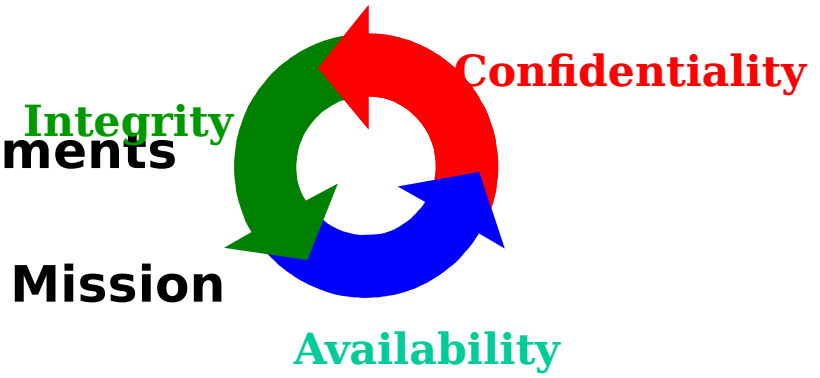
These security policies identify the Information Assurance/security requirements that must be addressed by:

- **Collateral Space**
- **Core Enterprise Services**
- **Horizontal Fusion Initiatives/Capabilities**
- **SIPRNET Backbone**
- **DoD/IC Facilities/Sites**

HORIZONTAL FUSION

Targeted Security Requirements

- **Based on DCID 6/3 and DoDI 8500.2**
- **For DCID 6/3 goal is to meet Protection Level 5 (PL5) requirements**
- **For DoDI 8500.2 goal is to meet Mission Assurance Category II and Confidentiality Level High requirements**
- **For FY04 we will achieve PL3 with some PL4 and PL5 compliance within some areas**



HORIZONTAL FUSION

Confidentiality Controls (1)

- **Provide Access Control through:**
  - **Metadata tag (with Classification Attribute) is applied to all objects**
  - **Digital signature is applied to object and tag**
  - **Changes to the Metadata tag are audited**
  - **The NCES Policy Decision Server and GDS/Extended LDAP will contain a Trusted Source of Clearance Information**
  - **Objects will use the classification attribute as an access control through the Role Base Access Control (RBAC) Filter**
- **Audits significant events and use audit analysis tools**
- **Uses DoD PKI for strong Identification and Authentication**
- **All data is labeled with classification and accesses using DDMS/IC Meta Data tagging**
- **Firewalls and IDS systems will be used for boundary defense**

HORIZONTAL FUSION

Confidentiality Controls (2)

- **Will use encryption (Type I certified and FIPS 140-2 validated) as needed to tunnel data through communications lines of lower or different classification levels or enclaves, (i.e., will tunnel Secret through NIPRnet to SIPRnet)**

- **System Assurance:**
  - **Will use system vulnerability tools (i.e., ISS, APPscan) to assure the continued integrity of security support structure**
  - **Will perform malicious code checking and mobile code verification**
  - **System Security Authorization Agreement (SSAA) includes: Security Requirements Traceability Matrices, Test plans, Test result reports, and System Documentation (e.g., User Manuals, CONOPS, System Administration Manuals)**
  - **Certification Testing will be conducted at SPAWAR Systems Center - Charleston**
  - **Test results will be reported to the DAA**

- **DoD CIO appointed DIA as the HF enterprise level DAA**

HORIZONTAL FUSION

Integrity Controls (1)

- Will do Systems and Data Backups
- Will have a CM plan
- Malicious code checking at data source
- Uses digital signatures to ensure data integrity
- System design includes best security practices (e.g., PK enabling of initiatives)
- Used applicable Security guidance documents
- Have a functional architecture for HF that defines external interfaces, protection mechanisms, user roles
- System will be accredited prior to implementation

HORIZONTAL FUSION

Integrity Controls (2)

- DoD PKI is used for digital signatures
- Use of Mobile code will be controlled
- DoD PKI used for Identification and Authentication
- Host Based IDS systems are used
- Role Based Access Control is used to control privileged accounts
- Use transmission integrity controls such as parity checks, labels, and encryption to prevent data corruption in transit
- Audit data is protected

HORIZONTAL FUSION

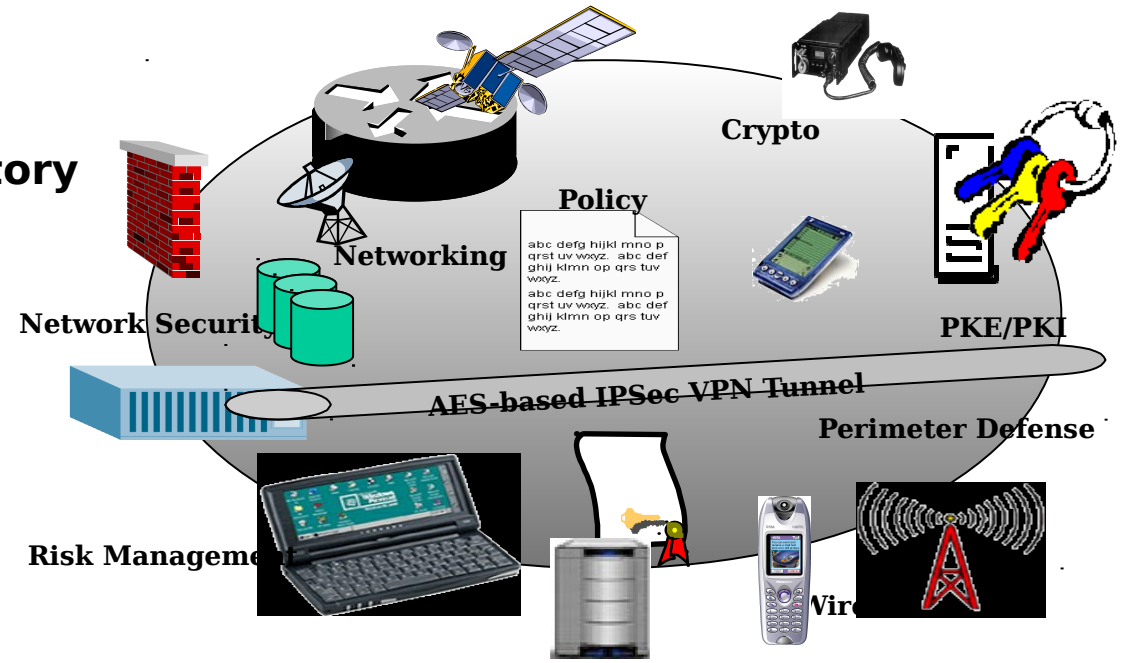
Availability Controls

- **Backups will be positioned to allow rapid recovery of the system**
- **Functional and compliance testing performed prior to deployments**
- **Hardware baseline is documented in the SSAA**
- **Public Domain software use is controlled**
- **DAA and other IA roles assigned**
- **Virus checking implemented on hardware**
- **Wireless computing is implemented in accordance with applicable Wireless policy DoDD8100.2**
- **Use vulnerability assessment tools to manage vulnerabilities**

HORIZONTAL FUSION

Key Security Technologies: A Diverse Set of Tools

- **Core Enterprise Security Services**
- **DDMS / IC Meta Data Tags**
- **GDS / Extended LDAP Directory**
- **SAML / XACML**
- **Role Based Access Control (RBAC)**
- **DoD PKI and Public Key Certificates**
- **AES and FIPS140-2 Cryptography**



HORIZONTAL FUSION

Standard Specifications as Guidance in the Development

User/Admin Interfaces

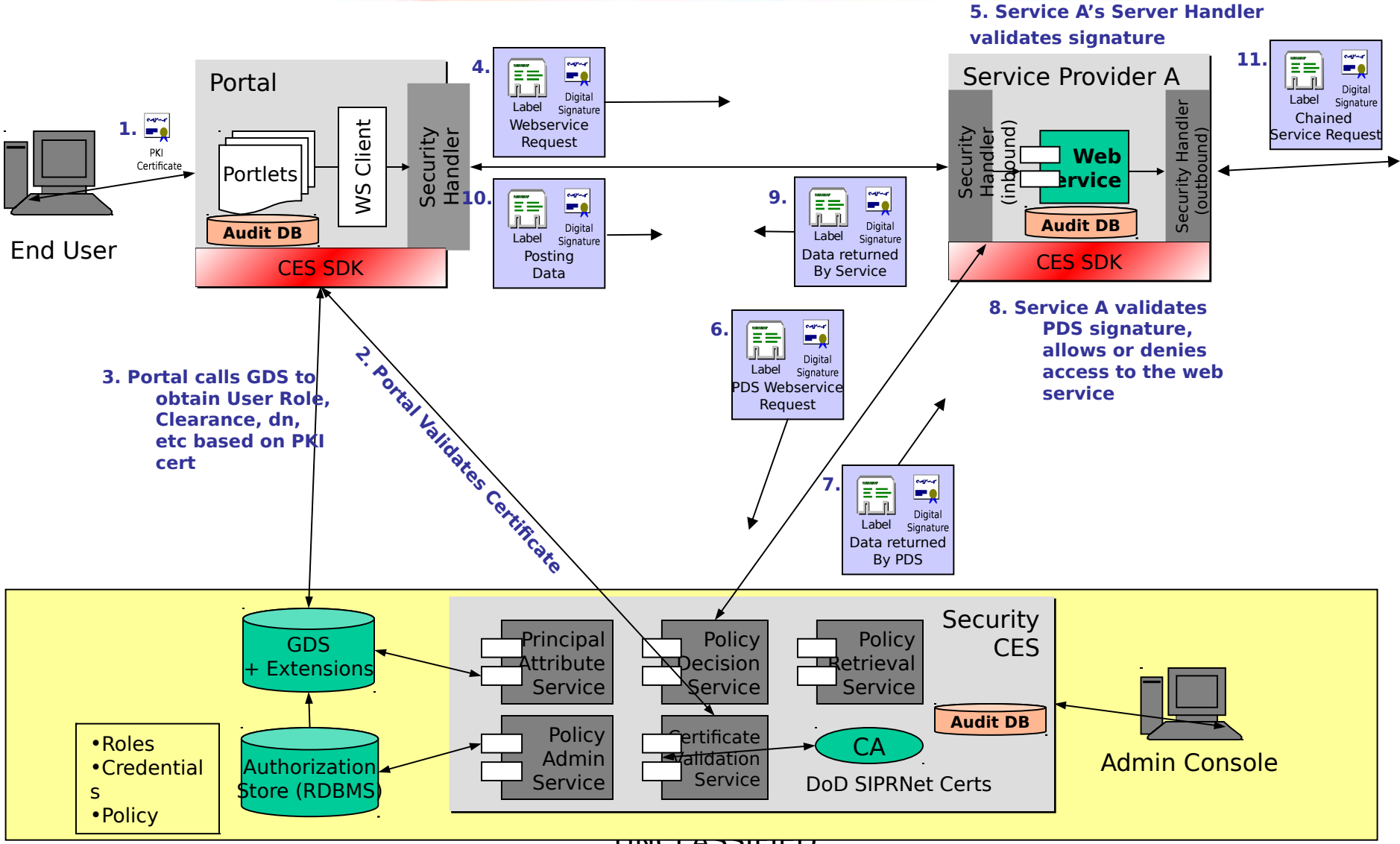
- **Cross-platform/browser (HTML 3.2/4.0; DHTML; CSS 1.0)**
- **JSR 168 Portlet/JSR 170 Specification**
- **JDK 1.4.2**
- ***Limited* JavaScript**
- **Web Services for Remote Portal (WSRP)**
- **Accepts XML/XSLT**
  - **Automatic rendering in portlet**
- **SAML/XML Signature/Encryption**
- **PKI and Directory Services**
- **Syndication (RSS v1.0)**
- **DDMS and IC Metadata Framework**

Middleware and Data Layers

- **XML & XML Schema v1.0**
- **Semantic Web Markup Languages (DAML, OWL)**
- **Registry standards (RDF/UDDI v2, JAXR)**
- **Web Services (WSDL v1.1, SOAP v 1.1), and JSR170**
- **J2EE (EJB, JAX Pack, JNDI, JMS)**
- **ODBC/JDBC**
- **SAML, XACML**
- **SQL database engines**
- **Syndication (RSS v1.0)**
- **XMPP**
- **JDK 1.4.2**
- **DDMS and IC Metadata Framework**
  - **Domain Namespaces**
  - **Content tagging**
  - **Taxonomies (categories)**
  - **Ontologies (relationships)**

HORIZONTAL FUSION

Conceptual Security Architecture



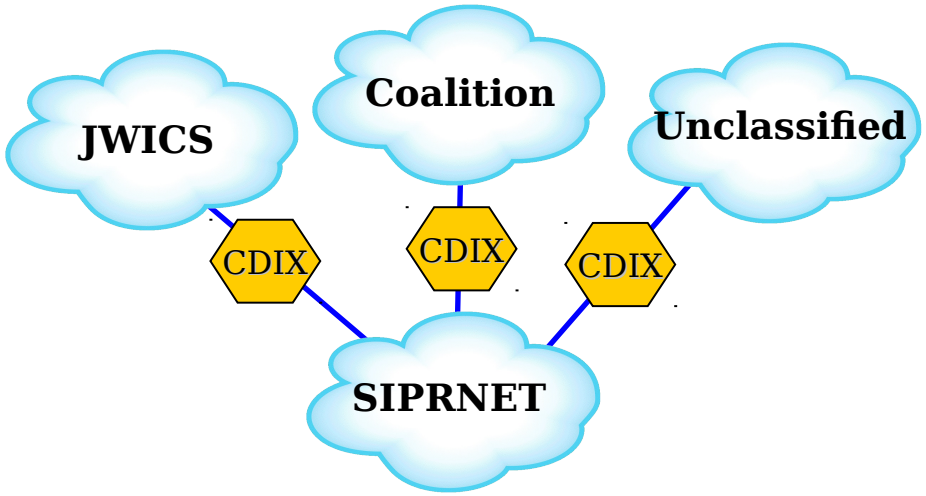
HORIZONTAL FUSION

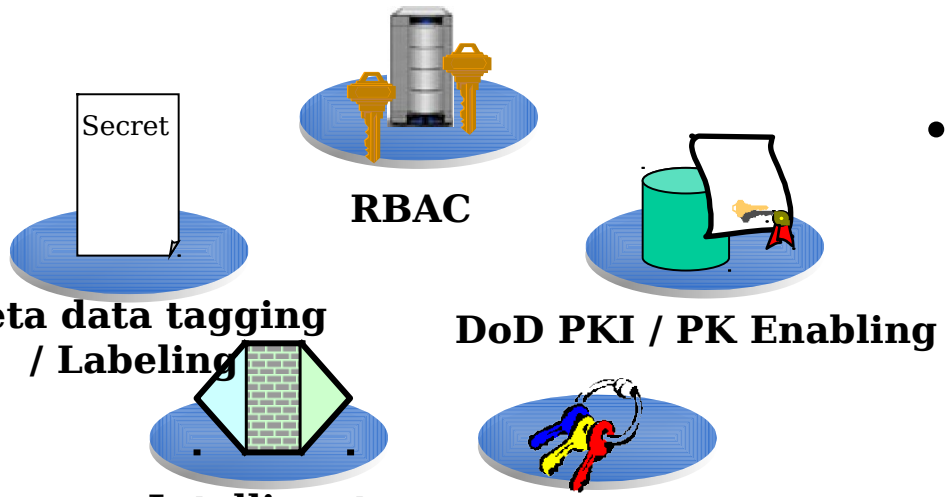
Secure Wireless

- **Mobile and wireless technologies – are burgeoning in the private sector. Wi-Fi, MANETS, 802.16, 3G, PDAs, and SDR are only a few.**
- **These technologies could bring enormous benefits to today's warfighter**
- **These "constrained" technologies are often space, power, CPU and bandwidth limited**
- **Moreover, due to the broadcast nature of the radio technology, the smaller size, and the mobility – challenging security issues exist**
- **Horizontal Fusion must leverage secure wireless nevertheless**

HORIZONTAL FUSION

Cross-Domain Information Exchange

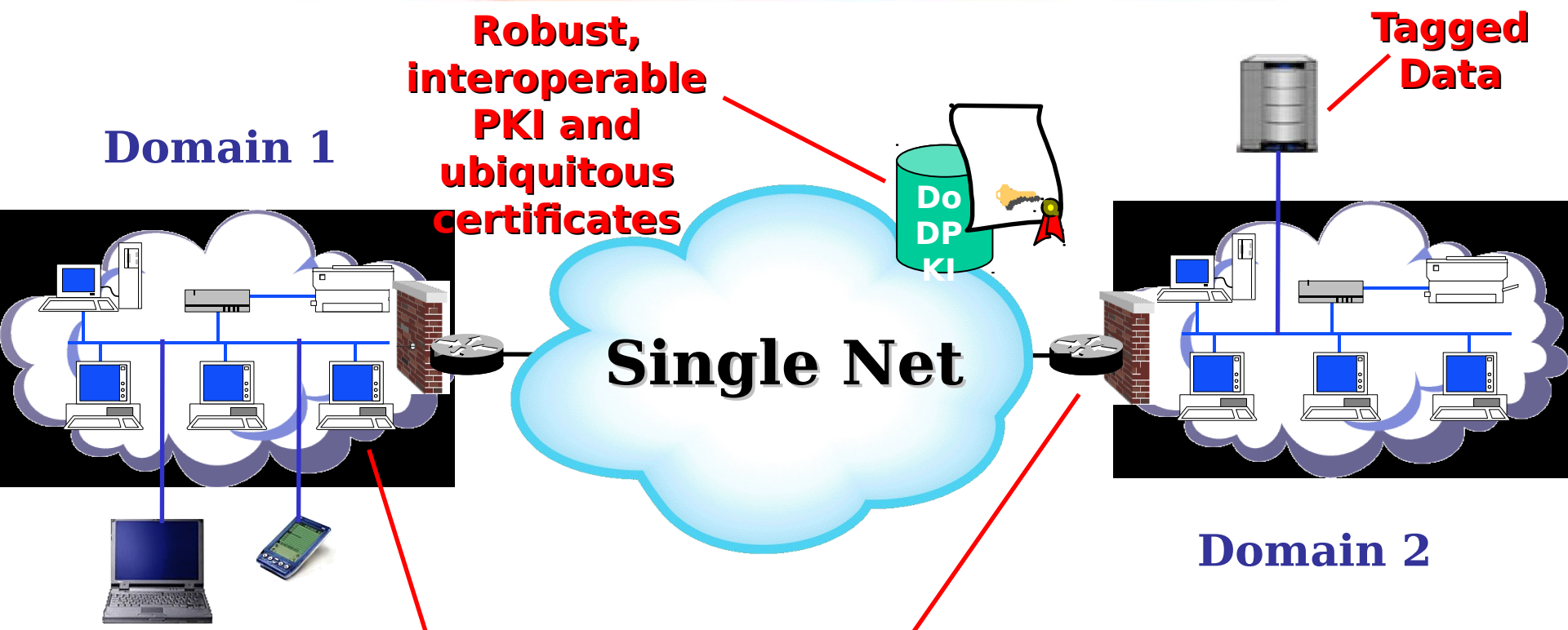




- Crossing multiple security domains is vital to our efforts
- Getting valuable information between the Collateral Space and the warfighter at the “pointy edge of the spear” is critical
- Bidirectional communication with Coalition Forces is essential
- Historical methods – using antiquated solutions are no longer acceptable in the emerging NetCentric DoD
- Service Oriented Architecture with built-in security features provides the foundation

HORIZONTAL FUSION

FY05 and Beyond



HORIZONTAL FUSION

Summary

- **Horizontal Fusion is truly a Catalyst for Net-centricity for the DoD**
- **Uses current standards adapted to a Net-centric environment**
- **Security features are diversified and embedded throughout the architecture**
- **Architecture and IA will continuously evolve with constant improvement**
- **Information Assurance implementation lessons-learned will be shared widely**